ATTACHMENT A
Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

1.(Currently Amended) A device ~~(30)~~ for connection to a data processing apparatus ~~(10)~~, the device including

authentication storage means ~~(12)~~ operatively coupled thereto for storing predetermined authentication information respective to a user,

the authentication storage means ~~(12)~~ being registered with a telecommunications system ~~(16)~~ which includes authenticating means ~~(18;102)~~ and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means ~~(12)~~, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means ~~(18;102)~~ to carry out the authentication process via a communication link ~~(19)~~ with the authenticating means ~~(18;102)~~ in the said telecommunications system ~~(16)~~ whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means ~~(12)~~,

the predetermined authentication information stored by the authentication storage means ~~(12)~~ corresponding to information which is used to authenticate the user registered with the telecommunications system ~~(16)~~ in relation to use of that user's telecommunications terminal in the telecommunications system ~~(16)~~.

2. (Currently Amended) The device of claim 1, comprising security data entry means ~~(46)~~ for obtaining security data independently of the data processing apparatus ~~(10)~~, and

means for analysing the entered security data for determining whether to allow access to the predetermined information.

3. (Currently Amended) The device of claim 2, wherein the security data entry means ~~(46)~~ comprises alphanumeric data entry means.

4. (Currently Amended) The device of claim 2 ~~or 3~~, wherein the security data entry means ~~(46)~~ comprises a keypad.

5. (Currently Amended) The device of claim 2,~~3 or 4,~~ wherein the security data comprises a Personal Identification Number (PIN) and the analysing means compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

6. (Currently Amended) The device of ~~any one of the preceding~~ claims 1, comprising a display ~~(48)~~ for displaying security information.

7. (Currently Amended) The device of ~~any one of the preceding~~ claims 1, comprising a data processing module ~~(36)~~ for controlling the communication with the data processing apparatus ~~(10)~~.

8. (Currently Amended) The device of claim 7, wherein the data processing module ~~(36)~~ of the device ~~(30)~~ is configured for communicating with a corresponding data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

9. (Currently Amended) The device of claim 8, wherein communication between the authentication storage means ~~(12)~~ and the data processing apparatus ~~(10)~~ is performed via the respective data processing modules ~~(36,38)~~.

10. (Currently Amended) The device of claim 7,~~8 or 9,~~ wherein the data processing module ~~(36)~~ of the device ~~(30)~~ includes means for decrypting encrypted data received from the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

11. (Currently Amended) The device of claim 7,~~8,9 or 10,~~ wherein the data processing module ~~(36)~~ of the device ~~(30)~~ includes means for encrypting data transmitted to the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

12. (Currently Amended) The device of claims 10 ~~or 11~~, wherein the respective data processing modules ~~(36,38)~~ comprise a key for allowing encryption and/or decryption of data.

13. (Currently Amended) The device of claim 12, wherein the key comprises a shared secret key for each of the respective data processing modules ~~(36,38)~~.

14. (Currently Amended) The device of ~~any one of~~ claims 1 ~~to 13~~, in which each user is authenticated in the telecommunications system by means of ~~the~~ use of a ~~smart card or~~ subscriber identity module ~~(e.g. SIM)~~, and in which the authentication storage means ~~(12)~~ respective to that user corresponds to or simulates the subscriber identity module ~~smart card~~ for that user.

15. (Currently Amended) The device of ~~any one of~~ claims 1 ~~to 14~~, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

16. (Currently Amended) The device of ~~any one of~~ claims 1 ~~to 15~~, in which the authentication storage means ~~(12)~~ is specific to that device ~~(30)~~.

17. (Currently Amended) The device of ~~any one of~~ claims 1 ~~to 16~~, in which the authentication process involves the sending of a message and the generation of a response

dependent on the message and the predetermined information.

18. (Currently Amended) The device of ~~any one of~~ claims ~~14 to 17~~, wherein the telecommunications system (16) includes means for levying a charge for the transaction when authorised.

19. (Currently Amended) The device of ~~any one of the preceding~~ claims ~~1~~ 1 in combination with the data processing apparatus ~~(10)~~.

20. (Currently Amended) The device of ~~any one of the preceding claims~~ claim 1 in combination with the telecommunications system ~~(16)~~.

21. (Currently Amended) A method for authenticating a transaction with data processing apparatus ~~(10)~~ in which the data processing apparatus ~~(10)~~ has operatively associated with it a security device ~~(30)~~ which in turn has operatively associated with it authentication storage means ~~(12)~~ for storing predetermined authentication information respective to a user,

the authentication storage means ~~(12)~~ being registered with a telecommunications system ~~(16)~~ which includes authenticating means ~~(18;102)~~ and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means ~~(12)~~, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means ~~(18;102)~~ to carry out the authentication process via a communication link ~~(19)~~ with the authenticating means ~~(18;102)~~ in the said telecommunications system ~~(16)~~ whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means ~~(12)~~, the predetermined authentication information stored by the authentication storage means ~~(12)~~ corresponding

to information which is used to authenticate the user registered with the telecommunications system ~~(16)~~ in relation to use of that user's telecommunications terminal in the telecommunications system ~~(16)~~,

the predetermined authentication information being obtained from the authentication storage means ~~(12)~~ via the security device ~~(30)~~ which controls access to the predetermined authentication information.

22. (Currently Amended) The method of claim 21, comprising obtaining security data independently of the data processing apparatus ~~(10)~~, and analysing the security data for determining whether to allow access to the predetermined information.

23. (Currently Amended) The method of claim 22, wherein the security data is obtained by alphanumeric data entry means ~~(46)~~.

24. (Currently Amended) The method of claim 21 ~~or 23~~, wherein the alphanumeric data entry means (46) comprises a keypad.

25. (Currently Amended) The method of claim 22~~,23 or 24~~, wherein the security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means (12) and only allows access to the predetermined information when the respective PINs match.

26. (Currently Amended) The method of ~~any one of~~ claims 21 ~~to 25~~, comprising displaying security information.

27. (Currently Amended) The method of ~~any one of~~ claims 21 ~~to 26~~, wherein communication with the data processing apparatus is controlled by a data processing module ~~(36)~~.

28. (Currently Amended) The method of claim 27, wherein the data processing module ~~(36)~~ of the device ~~(30)~~ is configured for communicating with a corresponding data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

29. (Currently Amended) The method of claim 28, wherein communication between the authentication storage means ~~(12)~~ and the data processing apparatus ~~(10)~~ is performed via the respective data processing modules ~~(36,38)~~.

30. (Currently Amended) The method of claim 27,~~28 or 29~~, wherein the data processing module ~~(36)~~ of the device ~~(30)~~ decrypts encrypted data received from the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

31. (Currently Amended) The method of claim 27,~~28,29 or 30,~~ wherein the data processing module ~~(36)~~ of the device ~~(30)~~ encrypts data transmitted to the data processing module ~~(38)~~ of the data processing apparatus ~~(10)~~.

32. (Currently Amended) The method of claim~~s~~ 30 ~~and 31~~, wherein the respective data processing modules ~~36,38~~ comprise a key for allowing encryption and/or decryption of data.

33. (Currently Amended) The method of claim 32, wherein the key comprises a shared secret key for each of the respective data processing modules ~~(36,38)~~.

34. (Currently Amended) A method according to ~~any one of~~ claim~~s~~ 21 ~~to 33~~, in which each user is authenticated in the telecommunications system ~~(16)~~ by means of ~~the~~ use of a ~~smart card or~~ subscriber identity module ~~(e.g. SIM)~~, and in which the authentication storage means respective to that user corresponds to or simulates the ~~smart card~~ subscriber identity module for that user.

35. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 34~~, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

36. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 35~~, in which each authentication storage means ~~(12)~~ is associated with a specific security device ~~(30)~~.

37. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 36~~, in which the authentication storage means ~~(12)~~ is associated with the data processing apparatus ~~(10)~~ by being associated with data or software for use by that data processing apparatus ~~10)~~.

38. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 39~~, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

39. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 40~~, including the step of levying a charge for the transaction when authenticated.

40. (Currently Amended) A method according to claim 39, in which the step of levying the charge is carried out by the said telecommunication system ~~(16)~~.

41. (Currently Amended) A method according to ~~any one of~~ claims 21 ~~to 40~~, in which the data processing apparatus ~~(10)~~ is a personal computer.

42. (Currently Amended) A device including authentication storage means ~~(12)~~ for controlling access to predetermined authentication information stored on the authentication storage means ~~(12)~~,

the device including means for coupling the device to a data processing apparatus ~~(10)~~ to

allow the authentication information to be used to authenticate a transaction performed by the data processing apparatus ~~(10)~~,

the predetermined authentication information stored on the authentication storage means ~~(12)~~ being respective to a user, the authentication storage means ~~(12)~~ being registered with a telecommunications system ~~(16)~~ which includes authenticating means ~~(18;102)~~ and for which the user has a telecommunications terminal,

the device, when operatively coupled to the authentication storage means ~~(12)~~, being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means ~~(18;102)~~ to carry out the authentication process via a communication link ~~(19)~~ with the authenticating means ~~(18;102)~~ in the said telecommunications system ~~(16)~~ whereby to authenticate the transaction by the user with the data processing apparatus, and

wherein security means is provided for controlling access to the authentication information via the data processing apparatus.

43. (Currently Amended) The device of claim 42, wherein the security means comprises means ~~(46)~~ for obtaining security data from a user and means for checking the validity of the security data and only allowing access to the authentication data if the security data is valid.

44. (Currently Amended) The device of claim 42 ~~or 43~~, wherein the security means comprises data processing means ~~(36)~~ for receiving an encrypted authentication request, encrypted using a predetermined key, from the data processing apparatus ~~(10)~~ and for decrypting the request.

45. (Currently Amended) The device of claim 44 in combination with the data processing apparatus ~~(10)~~, wherein the data processing apparatus ~~(10)~~ comprises means

for encrypting the authentication request using said key.

46. (Currently Amended) A device according to ~~any one of~~ claims ~~1 to 20 or 42 to 45~~, wherein the device ~~(30)~~ communicates wirelessly to authenticate the transaction.

47. (Currently Amended) A device according to claim 14, wherein the ~~smart card or SIM~~ subscriber identity module authenticates the transaction when the ~~smart card or SIM~~ subscriber identity module is operable in a mobile terminal.

48. (Currently Amended) A device according to claim 14, wherein the ~~smart card or SIM~~ subscriber identity module is further operable to authenticate a mobile terminal for use in the system.

49. (Currently Amended) A method according to ~~any one of~~ claims ~~21 to 41~~, wherein the security device ~~(30)~~ communicates wirelessly to authenticate the transaction.

~~51.~~50. (Currently Amended) A method according to claim 34, wherein the ~~smart card or SIM~~ subscriber identity module authenticates the transaction when the ~~smart card or SIM~~ subscriber identity module ~~-~~is operable in a mobile terminal.

51. (Currently Amended)A method according to claim 34, wherein the ~~smart card or SIM~~ subscriber identity module is further operable to authenticate a mobile terminal for use in the system.

52. (New) The method of claims 31, wherein the respective data processing modules comprise a key for allowing encryption and/or decryption of data.

53. (New) A device according to claim 42, wherein the device communicates wirelessly to authenticate the transaction.